Commonwealth of Massachusetts
Information Technology Division

Enterprise Wireless Security Standards: Wireless Personal Area Networks Version 1.1

This document identifies standards to ensure secure deployment, use and administration of Wireless Personal Area Networks (WPAN) by Commonwealth entities. Entities considering deployment of these technologies should first consult the Enterprise Wireless Security Policy. Entities covered by this policy must adhere to the standards detailed in this document for all WPAN deployments.

This document is one of the following Enterprise Wireless Security Standards documents that address major categories of wireless technology implementation:

- Wireless Mobile Communications (WMC)
- Wireless Local Area Networks (WLAN)
- Wireless Wide Area Networks (WWAN)
- Wireless Personal Area Networks (WPAN)

Additional references that entities may find useful as they plan wireless communications deployments are listed at the end of this document.

Wireless Personal Area Networks (WPAN)

Wireless Personal Area Networks (WPAN) utilize unlicensed frequencies for data communication between small devices over a limited distance. Typical WPAN include Bluetooth and InfraRed (IR). They are used, for example, to wirelessly interconnect a keyboard to a computer, a computer to a projector, a PDA to a notebook computer, or to communicate among PDAs. Bluetooth supports data transmission rates of up to 720Kbps at distances of up to 30 feet. As this technology matures, both transmission speed and range are expected to increase, with distances approaching 100 feet.

Since personal area networks are relatively new, a market for robust security solutions is only now emerging. For this reason, Commonwealth security standards for personal area networks are restrictive. No confidential data as defined by the entity may be transmitted over WPAN and devices may not connect directly to the Commonwealth or entity LAN or to MAGNet via WPAN without express approval of the Executive Department CIO, subsequent to a recommendation from the Enterprise Security Board. Data that is not confidential data may be transmitted via WPAN, but users should be aware that such transmission may be intercepted anywhere around, above or below the device, within the WPAN transmission range.

1. Acceptable Use Standards (WPAN)

A. No transmission of confidential data via WPAN
Because authentication and encryption products for WPAN networks and devices are still immature, no confidential data, as defined by the entity, may be transmitted via WPAN. Entities with WPAN applications that require transmission of confidential data may apply to the Enterprise Security Board for a variance to this standard if robust encryption and authentication can be demonstrated.

B. No LAN or MAGNet access via WPAN
Devices may not connect directly to the Commonwealth or entity LAN or to MAGNet via WPAN. Entities with WPAN applications that require LAN access may apply to the Enterprise Security Board for a variance to this policy if robust encryption and authentication can be demonstrated and devices can be protected through regular software upgrades, personal firewall and anti-virus software.

2. Infrastructure Standards (WPAN)

A. Registration of devices
Entities must require registration of each wireless device prior to the device being authorized to utilize WPAN communication with other devices. Entities must record serial numbers, phone numbers, MAC address, etc. as appropriate and obtainable for each wireless communications device.

B. 'WPAN to LAN' bridges not allowed
Devices must not be allowed to bridge WPAN and LAN or WLAN communications, nor are WPAN access points or bridges allowed on the Commonwealth or entity LAN or MAGNet.

3. Authentication and Encryption Standards (WPAN)

A. Local caching, storing and printing
Entities must be aware that local storing, caching or printing of confidential data on remote devices may pose a significant data security risk. Entities must advise users that confidential data as defined by the entity cannot be stored on the devices unless strongly encrypted. Entities should develop local policy as required to address this potential risk, in compliance with the Commonwealth's enterprise security policies as published by ITD, and relevant data confidentiality acts such as HIPAA, FIPA, or FERPA, based on the type of data involved.

B. Authentication of devices
Devices that may contain confidential data must have a first tier authentication for device access – either a password or PIN (personal identification number), or equivalent, such as a biometric (fingerprint scanner), voice recognition, etc. This first tier authentication helps to protect any data physically stored on the device.

4. Device Configuration and Security Standards (WPAN)

The portability and opportunity for loss/misplacement/theft of WPAN devices (such as PDAs and notebook computers) mandates that strong measures be utilized to protect any data on the devices as well as the devices themselves.

A. Protection of connected devices
All wireless devices that are connected in any way (wireless or wired such as synching files between a PDA and a networked device via cradle or other wired mechanism) to any computer or device on the Commonwealth LAN/MAGNet must be configured in compliance with the Commonwealth's enterprise security policies as published by ITD. Devices must be fully updated and patched, and

must run personal firewall and anti-virus software, if available for the device in compliance with Commonwealth and entity policies.

B. Ownership of connected devices
All devices that connect directly or indirectly to the Commonwealth LAN/MAGNet must be the property of the Commonwealth. No personally owned wireless Personal Area Network communications devices or vendor equipment may connect without express written permission of the Executive Department CIO, subsequent to a recommendation from the Enterprise Security Board. Commonwealth entities may apply for variances to this ownership requirement on an application-specific basis.

All users of WPAN connected devices must complete and sign a user acceptance agreement, similar to current VPN user acknowledgement, allowing ITD and their entity to scan/monitor and periodically audit the device. The user acknowledgement form must state that no one other than the authenticated user can use the device. Users of non Commonwealth-owned devices who have been approved for such use by the Executive Department CIO must complete the same user agreement noted above.

C. Disable auto-connection between devices
Devices must be configured so that connections to other devices are rejected without express authorization of the device user.

D. Physical security of remote devices
Entities must develop policies regarding physical security of portable IT devices, including procedures to prevent theft or loss and to report theft or loss in the event of such occurrence.

Additional Reference

National Institute of Standards and Technology (NIST) Special Publication 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices", by Tom Karygiannis and Les Owens, November 2002.